

This AGREEMENT is entered into by and between the MNSure Board on behalf of the State of Minnesota ("MNSure" or "State") and OptumInsight, Inc. and its affiliate QSSI (collectively, "Optum").

WHEREAS, MNSure requires certain expertise to assist in the evaluation of establishing and implementing MNSure's technical infrastructure programs;

WHEREAS, Optum is willing to provide such assistance to MNSure; and

WHEREAS, MNSure is authorized under Minnesota Statutes, section 62V.05, subdivision 1, paragraph b to seek and accept donations and services to assist in the operation of MNSure and to enter into agreements for services.

## AGREEMENT

### 1. Term of Agreement

1.1 **Effective date:** January 7, 2013 or the date the State obtains all required signatures, whichever is later.

1.2 **Expiration date:** March 15, 2014, or until all obligations have been satisfactorily fulfilled, whichever comes first.

### 2. Duties

2.1 MNSure shall:

2.1.1 Provide available functional staff and subject matter expertise as requested by Optum for initial assessment meetings and any follow-up discussions as needed.

2.1.2 Provide appropriate and supportive content and artifacts in support of the Optum assessment.

2.2 Optum shall:

2.2.1 Perform an End-to-End Technology Software and Data Analysis Assessment and provide a written recommendation and estimate for proposed next steps.

2.2.2 Provide a Program Governance and Structure Assessment and provide a written recommendation and estimate for proposed next steps.

2.2.3 Provide a Contact Center Assessment and provide a written recommendation and estimate for immediate augmented staffing and workflow improvements.

### 3. Authorized Representative

MNSure's Authorized Representative is Scott Leitz, MNSure Chief Executive Officer.

Optum's Authorized Representative is James Eppel.

### 4. Amendments

Any amendment to this agreement must be in writing and will not be effective until it has been executed and approved by the same parties who executed and approved the original agreement, or their successors in office.

## **5. State Audits**

As required by law, Optum's books, records, documents, and accounting procedures and practices directly relevant to this Agreement are subject to examination by MNSure and/or the Legislative Auditor, as appropriate, for a minimum of six years from the end of this Agreement.

## **6. Property**

MNSure shall own the documents to be delivered to MNSure as described in Section 2.2, and shall have the right to use, reproduce, and disclose data and information contained in those documents subject to any applicable limitations provided for under the Minnesota Government Data Practices Act, Minnesota Statutes, Chapter 13, including the limitations on disclosing trade secret information in Minn. Stat. § 13.37.

Optum represents and warrants that the documents described above do not and will not infringe upon any intellectual property rights of other persons or entities.

## **7. Information Privacy and Security**

**7.1 Information Covered by this Provision.** In carrying out its duties, Optum will be handling one or more types of private information, collectively referred to as "protected information," concerning individual State clients. "Protected information," for purposes of this agreement, includes any or all of the following:

- (a) Private data (as defined in Minn. Stat. §13.02, subd. 12), confidential data (as defined in Minn. Stat. §13.02, subd. 3), welfare data (as governed by Minn. Stat. §13.46), medical data (as governed by Minn. Stat. §13.384), and other non-public data governed elsewhere in the Minnesota Government Data Practices Act (MGDPA), Minn. Stats. Chapter 13;
- (b) Protected health information ("PHI") (as defined in and governed by the Health Insurance Portability Accountability Act ["HIPAA"], 45 CFR § 164.501);
- (c) Federal Tax Information ("FTI") (as defined by 26 U.S.C. § 6103);
- (d) Records (as defined by the Privacy Act of 1974, 5 U.S.C. § 552a); and
- (e) Other data subject to applicable state and federal statutes, rules, and regulations affecting the collection, storage, use, or dissemination of private or confidential information

**7.2 State Duties Relating to Protection of Information.** State shall:

- (a) Only release information which it is authorized by law or regulation to share with Optum.
- (b) Obtain any required consents, authorizations, or other permissions that may be necessary for it to share information with Optum.
- (c) Notify Optum of limitations, restrictions, changes, or revocation of permission by an individual to use or disclose protected information, to the extent that such limitations, restrictions, changes or revocation may affect Optum's use or disclosure of protected information.
- (d) Not request Optum to use or disclose protected information in any manner that would not be permitted under law if done by State.

**7.3 Optum Duties Relating to Protection of Information.** Optum shall:

- (a) Be responsible for ensuring proper handling and safeguarding by its employees, subcontractors, and authorized agents of protected information collected, created, used, maintained, or disclosed on behalf of State. This responsibility includes applying appropriate screening measures and monitoring to protect information privacy, ensuring that employees and agents comply with and are properly trained regarding, as applicable, the laws listed above in paragraph 10.1, and having implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the

confidentially, integrity, and availability of any electronic protected health information at rest and in transit that it creates, receives, maintains, or transmits on behalf of State.

(b) Comply with the "minimum necessary" access and disclosure rule set forth in the MGDPA. The collection, creation, use, maintenance, and disclosure of protected information shall be limited to that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government. Minn. Stat. § 13.05 subd. 3.

(c) Report to State any privacy or security incident regarding the information of which it becomes aware. For purposes of this Contract, "Security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Privacy incident" means violation of the Minnesota Government Data Practices Act (MGDPA) and/or the including, but not limited to, improper and/or unauthorized use or disclosure of protected information, and incidents in which the confidentiality of the information maintained by it has been breached. This report must be made in writing and submitted to State immediately and in no case more than 7 days after learning of such incident.

(d) Unless provided for otherwise in this Contract, if Optum receives a request to release the information referred to in this Clause, Optum must immediately notify State. State will give Optum instructions concerning the release of the data to the requesting party before the data is released.

(e) Not use or further disclose protected information created, collected, received, stored, used, maintained, or disseminated in the course or performance of this Contract other than as permitted or required by this Contract or as required by law, either during the period of this Contract or hereafter.

(f) In accordance with Minn. Stat. § 62V.06, subd. 9, Optum may not sell any data collected, created, or maintained by State, regardless of its classification, for commercial or any other purposes.

(g) Consistent with this Contract, ensure that any agents (including contractors and subcontractors), analysts, and others to whom it provides protected information, agree in writing to be bound by the same restrictions and conditions that apply to it with respect to such information.

(h) To the extent that any protected information is PHI:

1. Comply with the minimum necessary rule and limit the collection, creation, use, maintenance, and disclosure of PHI to "that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government." See 45 C.F.R. §§ 164.502(b) and 164.514(d).

2. Report any breach or security incident pursuant to the HIPAA Privacy Rule (45 C.F.R. Part 164, Subpart E). This report must be in writing and sent to State not more than 7 days after learning of such non-permitted use or disclosure. Such a report will at least:

- A. Identify the nature of the non-permitted use or disclosure;
- B. Identify the PHI used or disclosed;
- C. Identify who made the non-permitted use or disclosure and who received the non-permitted or violating disclosure;
- D. Identify what corrective action was taken or will be taken to prevent further non-permitted uses or disclosures;
- E. Identify what was done or will be done to mitigate any deleterious effect of the non-permitted use or disclosure;
- F. Provide such other information, including any written documentation, as State may reasonably request; and

G. Provide notice required by 45 C.F.R. §§ 164.404 through 164.408 to affected individuals, news media, and/or the Office of Civil Rights, Department of Health and Human Services, only upon direction from and in coordination with the State.

3. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree in writing to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;
4. Within ten (10) business days of a request from an individual or their designee, make available protected health information in a designated record set, consistent with Minn. Stat. § 13.04, subd. 3, and 45 C.F.R. § 164.524;
5. Within ten (10) business days, forward any request to make any amendment(s) to protected health information in a designated record set to the State in order for the State to satisfy its obligations under Minn. Stat. § 13.04, subd. 3 and 45 C.F.R. § 164.526;
6. Document such disclosures of PHI and information related to such disclosures as would be required for State to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Maintain and make available no later than fifteen (15) days after receipt of request from the State, the information required to provide an accounting of disclosures to the State as necessary to satisfy the State's obligations under 45 C.F.R. § 164.528, or upon request from State respond directly to individual's request for an accounting of disclosures;
7. To the extent the business associate is to carry out one or more of State's obligation(s) under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to State in the performance of such obligation(s); and
8. Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.
9. Optum may not use or disclose protected health information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by State.
10. Comply with any and all other applicable provisions of the HIPAA Privacy Rule, Administrative, and Security Standards, including future amendments thereto. Develop written policies and procedures for safeguarding and securing PHI and complying with HIPAA and the HITECH Act, and other privacy laws.
11. Designate a privacy official to be responsible for the development and implementation of its policies and procedures as required by 45 C.F.R. Part 164, Subpart E.
  - (i) To the extent that any protected information is FTI, ensure that this data only be used as authorized under the Patient Protection and Affordable Care Act and the Internal Revenue Code, 26 U.S.C. § 6103(C), and restrict from use for any other purpose.
  - (j) Mitigate, to the extent practicable, any harmful effects known to it of a use, disclosure, or breach of security with respect to protected information by it in violation of this Contract.
  - (k) Report and mitigate any fraudulent activities;
  - (l) Comply with any and all other applicable provisions of the Final Exchange Privacy Rule at 45 C.F.R. § 155.260, including future amendments thereto.

**7.4 Disposition of data upon completion, expiration, or agreement termination** Upon completion, expiration, or termination of this Agreement, Optum will return to State or destroy all protected information received or created on behalf of State for purposes associated with this

Agreement. A written certification of destruction or return to Authorized Representative listed in Section 3 is required. Optum will retain no copies of such protected information, provided that if both parties agree that such return or destruction is not feasible, or if Optum is required by the applicable regulation, rule or statutory retention schedule to retain beyond the life of this Agreement, Optum will extend the protections of this Agreement to the protected information and refrain from further use or disclosure of such information, except for those purposes that make return or destruction infeasible, for as long as Optum maintains the information.

**7.5 Sanctions.** In addition to acknowledging and accepting the terms set forth in Section 10 of this Agreement, the parties acknowledge that violation of the laws and protections described above could result in limitations being placed on future access to protected information, in investigation and imposition of sanctions by the U.S. Department of Health and Human Services, Office for Civil Rights, and/or in civil and criminal penalties.

**7.6 Interpretation.** Any ambiguity in this Contract shall be resolved to permit the parties to comply with HIPAA, MDGPA, and other applicable state and federal statutes, rules, and regulations affecting the collection, storage, use and dissemination of private or confidential information.

## **8. Inapplicability of Certain Affordable Care Act Provisions**

The State understands that Optum and QSSI are 100% beneficially owned by UnitedHealth Group, which also owns 100% of UnitedHealthcare, a health insurance issuer. UHC does not participate in the State's health insurance exchange. The State represents and warrants that it has determined, and will obtain confirmation from HHS, that (1) the eligible entity provisions at 42 USC § 18031(f)(3) and 45 CFR § 155.110, and (2) the requirements set forth in 45 C.F.R. § 155.215, do not apply to this contract. The State expressly warrants that (1) the State will not prohibit or seek to prevent health insurance issuers affiliated with Optum and QSSI from participating in the State health insurance exchange as a result of the performance of work under this contract by Optum; and (2) it will obtain confirmation from HHS that HHS will not prohibit or seek to prevent health insurance issuers affiliated with Optum or QSSI from participating in any health insurance exchange as a result of the performance of work under this contract by Optum.

## **9. Mitigation of Organizational Conflicts of Interest.**

The State understands the relationship between Optum, QSSI, and UHC, and the work that the Optum team will perform under this Agreement. The scope of work under this Agreement includes reviewing the work performed to design and implement the MNsure System and MNsure operations to date, and making recommendations regarding more effective ways to implement the MNsure System and MNsure operations. Optum's recommendations in these areas could lead to future work for the Optum team to implement changes to the MNsure System or MNsure operations. MNsure represents and warrants that Optum's role in making recommendations under this Agreement will not create an OCI that would prevent MNsure from awarding Optum a follow-on contract to implement those recommendations, and if any such OCI is later identified MNsure will waive it. As noted above, UHC does not offer plans through MNsure, but it does participate in Medicaid programs. To mitigate any unequal access to information OCI that might arise with respect to UHC, the Optum team performing this Agreement will maintain information gained in performance of the the Agreement as confidential, and will disclose it only on a need-to-know basis. To mitigate any potential impaired objectivity OCIs, MNsure personnel will closely supervise the work that the Optum team performs under this Agreement. The State represents and warrants that it has accepted these measures as adequate to mitigate any OCIs, or that it will waive any remaining OCIs.

## **10. Limitation of Liability & Limitation of Warranty**

Neither party shall be liable to the other for any form of damages (whether direct, indirect, incidental, special, exemplary, punitive, consequential, or other) that may arise from either party's performance of,

or failure to perform, work under this Agreement. Optum makes no warranties or representations, express or implied, regarding its work under this Agreement, and specifically disclaims the warranties of merchantability and fitness for a particular purpose.

#### 11. Termination

Either party may terminate this agreement at any time, with or without cause, upon 30 days' written notice to the other party.

##### 1. MNSure

By: [Signature]  
(with delegated authority)

Title: Interim CEO

Date: 1-8-14

##### 2. Optum

By: [Signature]  
(with delegated authority)

Title: SVP, OptumInsight

Date: January 8, 2014